TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

HACKER JOURNAL

QUATTORDICINALE ANNO 3 - 21 OTTOBRE / 4 NOVEMBRE 2004 - SPED. IN ABB. POST. 70% - MILANO
www.hackerjournal.it N. 61

SKYPE e TELEFONI GRATIS

HACKMACHINE

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

Dove si **IMPARA** in fretta **A PROGRAMMARE**

Emmanuel Goldstein: **PROFESSOR HACKER**

NOVITÀ: MITICO POSTER IN REGALO!

Ricattatori on-line: sotto attacco i CASINÒ

9 771594 577001 40061

4ever

Anno 3 – N. 61
21 Ottobre / 4 Novembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

NON SA (quanto gli costa)

La cosa che costa di più in assoluto è non sapere le cose

Larry Ellison, fondatore di Oracle, al teatro Manzoni di Milano. Mi appare Daniela in videochat. Carina, Daniela. Non lo sapessi, mi perderei l'occasione. Chiede aiuto: il dock del suo iPod non funzionava bene. Quindi? (dico) Allora ho lanciato i test diagnostici dell'iPod (mi risponde). E adesso l'iPod non si accende più. Hmm. Perché la diagnostica dell'iPod, se era il dock a non funzionare? È come aggiustare lo schienale di una seggiola perché una gamba è più corta, non ha senso.

Mi risponde: non lo so. Va bene, cerchiamo di capire. Che test hai lanciato, esattamente? Non lo so, dice.

Dani, sei carina, ma se non sai proprio niente ti conviene portarlo a riparare. Certo, ti costerà. Se vuoi ti accompagno. Lo so, che sei carina, e l'occasione non la perdo.

MisterMyst l'ho incontrato a un raduno di gente Linux. Lui era lì per curiosità, visto che usa Windows. Chiede aiuto. Ha installato il Service Pack 2 di Windows. Bravo, penso, adesso hai il sistema un po' più sicuro. Viene fuori che si è preso un worm. Ma hai installato le patch di sicurezza? Ma come, fa lui, cento mega di update e devo ancora installare le patch? Eh sì. Ah, cavolo. Si rabbuia un attimo. Pensavo bastasse il Service Pack, dice. "Non sapevo"

Arnaldo ogni tanto si lascia tentare da un sito porno. Mi ha telefonato allarmato. Si è lasciato tentare un po' troppo e per una volta si è iscritto, per qualche dollaro al mese. Poi si è stufato e si è disiscritto. Solo che il sito se ne frega e continua ad addebitargli sulla carta di credito qualche dollaro ogni mese. Adesso ha telefonato alla società della carta di credito, ha fatto la denuncia, quei pochi soldi in sé non sono un problema, ma gli costerà un sacco di tempo e di noie. Brontola. "Se lo avessi saputo"

Così va il mondo. A sapere le cose si è avvantaggiati. Non saperle costa. Come minimo ci si perde un'uscita con Daniela.

Come si fa a sapere le cose? Facile. Si mette in moto il cervello. Si accende il browser. Si legge una rivista che te le spiega. Non sai quale possa essere? Lo sai, lo sai, siamo tutti qui apposta.

theguilty@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea: Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Copertina: Daniele Festa

Publishing company: 4ever S.r.l. Via Torino, 51 20063 Cernusco S/N (MI) Fax +39/02.92.43.22.35

Printing: Roto 3

Distributore: Parrini & C. S.PA. 00189 Roma - Via Vitorchiano, 81 Tel. 06.33455.1 r.a. 20134 Milano, V.le Forlanini, 23 Tel. 02.75417.1 r.a.

Abbonamenti: Staff S.r.l. Via Bodoni, 24 20090 Buccinasco (MI) Tel. 02.45.70.24.15 Fax 02.45.70.24.34 Lun. - Ven. 9,30/12,30 - 14,30/17,30 abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

O SI DOMINA O SI È DOMINATI!

Un diciannovenne tedesco porta lo scompiglio nell'amministrazione dei domini di eBay

La bandiera della Bassa Sassiona diventerà la bandiera degli hacker?

Secondo la polizia tedesca un ragazzo di 19 anni di Helmstedt, Bassa Sassonia, ha confessato il dirottamento del sito tedesco di eBay e ora rischia l'incriminazione per sabotaggio informatico.

Il dirottamento sarebbe avvenuto a fine agosto, quando i visitatori al sito eBay.de venivano appunto canalizzati su un DNS (Domain Name Server) diverso da quello giusto e di conseguenza non potevano partecipare alle aste che fanno la fortuna del sito (e di chi lo frequenta, se è bravo).

Il colpevole non sarebbe particolarmente esperto di computer e ha dichiarato di essersi semplicemente imbattuto in alcuni siti che spiegano come effettuare un dirottamento di DNS, dopo di che si è limitato a seguire le istruzioni.

A suon di provare

Il diciannovenne ha chiesto il trasferimento per ben più di un dominio: ci ha provato con Google.de, Web.de, Amazon.de e vari altri. La richiesta, come dovrebbe succedere normalmente, è stata respinta in tutti i casi tranne, per motivi ancora da chiarire, quello di eBay. In particolare la polizia sta cercando di capire come sia stato possibile farlo senza il consenso di qualcuno in eBay.

Per il momento la società temporeggia e vuole capire bene che cosa sia successo, prima di fare causa al ragazzo, che comunque rischia di suo un processo per sabotaggio informatico. Pare che la Bassa Sassonia sia proprio terra di hacker: sempre lì, lo scorso maggio, era stato individuato un altro adolescente accusato di avere creato il virus Sasser. E qualcuno si è messo in tasca 250 mila dollari da Microsoft per avere fatto la spia, ma questa è un'altra storia.

Nyarlathotep
nyarlathotep@hackerjournal.it

COME E PERCHÉ IL DNS HIJACKING

Abbiamo parlato di dirottamento di DNS, ma il termine hackeristico è DNS hijacking, appunto dirottamento. C'è anche chi dice DNS redirection.
Come un dirottatore prende il controllo di un aereo con l'intenzione di portarlo in luogo diverso dalla sua destinazione vera, così un dirottatore di DNS prende il controllo di una comunicazione tra due entità e si sostituisce a una di esse.
Un tipo di dirottamento è l'attacco man-in-the-middle: ci inseriamo nella comunicazione tra Pippo e Pluto e parliamo con Pluto facendo finta di essere Pippo, e con Pippo fingendoci Pluto. Un altro invece riguarda i browser, che credono di caricare una pagina da un sito e invece il sito è tutt'altro. Un ultimo tipo di dirottamento, meno hackeristico, consiste nel registrare un nome di dominio quasi uguale a quello di un altro sito. Così, se qualcuno sbaglia a digitare, finisce sul sito quasi gemello, che di solito è riempito di pornografia o schifezze assortite.

NEWS

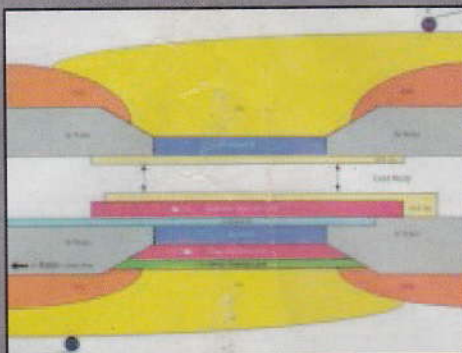
NO AL MONOPOLIO DEL NUOVO SKYBOX

La guerra del decoder prosegue, ma siamo agli sgoccioli. Sky sta vincolando gli utenti al proprio decoder NDS, "che complica senza alcuna ragione la possibilità di vedere i canali in chiaro che non rientrano nei pacchetti offerti dal monopolista". Così afferma il comunicato di Altroconsumo. Sky ha ribadito che concederà nei prossimi mesi la possibilità di allargare a 300 il numero di canali in chiaro "fuori pacchetto".
Ovviamente questa mossa non basta né ad Altroconsumo, né tantomeno a noi utenti. È come se un produttore televisivo, per di più in assenza di concorrenza, costringesse gli utenti all'acquisto di un televisore speciale ed esclusivo prodotto dalla stessa emittente. Cosa sta facendo l'Autorità garante delle Comunicazioni? Per ora, pare nulla.

PENA DI MORTE IN CINA

Martedì 14 Settembre 2004, l'agenzia cinese Xinhua ha diffuso la notizia che quattro cinesi sono stati fucilati per un reato di frode bancaria. Giusto per sapersi regolare, in Cina lo stato uccide per: avvelenamento di bestiame - omicidio - tentato omicidio - omicidio colposo - uccisione di una tigre - rapina a mano armata - rapina - stupro - ferimento - assalto - furto ripetuto - furto - intrusione - rapimento - traffico di donne o bambini - organizzazione della prostituzione - sfruttamento della prostituzione - organizzazione di spettacoli pornografici - pubblicazione di materiale pornografico - teppismo - disturbo dell'ordine pubblico - esplosioni provocate - distruzione o danneggiamento della proprietà pubblica o privata - sabotaggio controrivoluzionario - incendio - traffico di droga - corruzione - truffa - concussione - frode - usura - contraffazione - rivendita di ricevute IVA - evasione fiscale - furto o costruzione illegale di armi - possesso o vendita illegali di armi e munizioni - furto o contrabbando di tesori nazionali o reliquie culturali - spaccio di denaro falso – ricatto.

» UN TRANSISTOR SALVERÀ IL DISCO

All'Università di Oxford è in sviluppo un progetto di un nuovo tipo di transistor sensibile ai campi magnetici che lo attraversano, anche di debolissima intensità. Per chi costruisce i nostri hard disk pare che l'aggeggio possa essere come manna, perché sono sempre alla ricerca di dispositivi in grado di aumentare la quantità di dati scrivibili sui dischi, a parità di dimensioni.
Per di più si aprono prospettive anche per dispositivi di memoria non volatili, simili alle attuali Ram flash. Anche questo un progetto per il futuro, ma da come vanno le cose nel settore dell'elettronica, c'è da aspettarsi presto qualche pratico risultato.

» IL BOSONE DI HIGGS

Scusi, può ripetere? Ebbene sì, il bosone di Higgs è una particella della materia che stanno studiando al Cern di Ginevra e che, pare, sfugga all'osservazione pratica. Per cui il mondo della ricerca è in fermento perché sono riusciti a costruire otto bobine ciascuna di 5 per 25 metri, assemblate a 100 metri di profondità nella caverna che ospita il rivelatore di Atlas.
Il tutto in materiale superconduttore, s'intende, e quindi raffreddato a temperature di -268 gradi centigradi, ovvero prossime allo zero assoluto. Una sfida tecnologica che

HOT NEWS

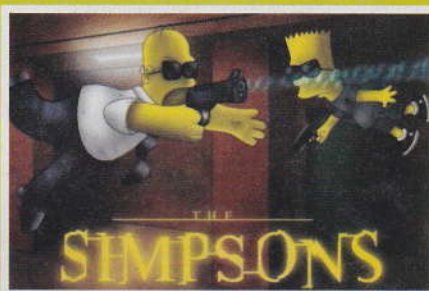
IN ARTE GOLDSTEIN, IN PRATICA ARRESTATO

Eric Corley aka Emmanuel Goldstein è stato fermato per 33 ore dalla polizia di New York per aver partecipato a una manifestazione contro la Convention repubblicana. Il nostro è stato fortunato per essere stato rilasciato senza conseguenze, visto che una causa persa qualche anno fa, intentata dalle case discografiche americane, lo aveva già visto sconfitto. Comunque, da anziano fondatore della rivista 2600 the hacker quarterly , ha scritto e fotografato quanto più poteva e ha messo tutto in linea: www.2600.com

BANDA LARGA NEL PAESE DEI TARTUFI

Provincia di Cuneo: la comunità montana dell'Alta Langa, capofila il paese di San Benedetto Belbo, attiva una rete wireless intercomunale per tutti i 21 comuni, un collegamento Internet in larga banda via satellite e la videosorveglianza centralizzata.

Così è nata la più grande rete intercomunale wifi d'Italia e uno dei primi esperimenti al mondo di copertura territoriale completa, oltre 200 km quadrati, tramite un sistema wireless. Bello, speriamo non rimanga isolato. Tutte le info qui: www.comune.sanbenedettobelbo.cn.it

TUTTO THE SIMPSONS SU UN MODS

I 350 episodi di The Simpsons, per un totale di 8.080 minuti, potrebbero tranquillamente starci sui nuovi dischi in tecnologia MODS che sta per Multiplexed Optical Data Storage. Sono ancora sperimentali, ma nei laboratori sono ormai una realtà e dimostrano di poter contenere fino a 1 TeraByte di dati, ovvero mille gigabyte. Come dire che la trilogia de "Il Signore degli Anelli" ci sta tutta tredici volte su un unico disco. Sono attesi sul mercato per il 2010, ma nel frattempo potremo accontentarci di una versione di DVD "BlueRay" da 25GB per lato, disponibile, si presume, per fine 2005.

IL POLITECNICO DI MILANO SU SKY

Si chiama "Mondo Politecnico" e va in onda sul canale 817. Sono sedici puntate di un'ora ciascuna, con tre passaggi in orario tardo pomeridiano e serale, che approfondiranno temi scientifici e di ricerca del Politecnico di Milano. La promessa è un tono "intrigante nella sua continua tensione a scoprire i retroscena del mondo della ricerca rivelando aneddoti e curiosità, senza perdere in rigore e autorità scientifica". Da vedere e giudicare.

nemmeno c'immaginiamo. A cosa serve? Ma a vedere in pratica il bosone di Higgs, perbacco!

LA MUSICA DIVENTA COLORE

Niente a che vedere con la fantasia di Windows Media Player

Fino a oggi trasporre il segnale musicale in immagini colorate è stato un gioco da ragazzi e quindi, si sa, in quanto gioco è assolutamente affidato al caso. Oggi, invece, il Politecnico di Milano ha depositato il brevetto del Musicolor, un apparecchio che associa la musica digitalizzata a precise e univoche mappe cromatiche dinamiche. Basato sulle stesse proprietà fisiche della materia è quindi immutabile e preciso e universale: un dato suono, una data cromia. Non si scappa. Il che ci pone anche una serie di nuovi interrogativi: cosa acca-

2 Mbit via satellite

Ho bisogno di sapere a quale gestore posso rivolgermi a riguardo i collegamenti internet tramite satellite, quali sono le componenti necessarie (kit) da acquistare , quali potrebbero essere i costi di attivazione/canoni annuali di gestione per una utenza non privata e se è prevista la possibilità da parte di altri utenti di collegarsi all'utente primario connesso via satellite attraverso rete wireless.

Antonio

Ecco due risposte: www.satlink.it e www.skylogic.it. Hanno esattamente la soluzione che cerchi, ci pare. Sono diverse le comunità montane o rurali in Italia che si stanno attrezzando in questo modo, così da evitare la necessità di Adsl, che non arriva dappertutto. Ovviamente sono soluzioni un po' più costose.

Pagefile.sys

Ho un problema: volevo sapere a cosa serve il file nascosto pagefile.sys, contenuto in C:\ (uso Win XP), visto che mi sono accorto che la sua dimensione raggiunge gli 800 Mbyte!

Neo88

È il file di "appoggio" del sistema operativo che tiene una specie di cache su disco di tutto quanto si sta facendo. Serve per rendere più veloci alcune operazioni, essendo di fatto usato come un'estensione (più lenta) della RAM.

È un francobollo con una buona risoluzione fatene buon uso, l'ho realizzato appositamente per Voi e siete liberi di stamparlo se Vi garba.

Cristian

Ci garba!

PRECISO, PRECISO

Hi numero 57 pag. 3, riquadro Jello Biafra - Kevin Mitnick...: Jello Biafra non è un rapper, ma punk fondatore dello storico gruppo dei Dead Kennedys ;)))

claudio

Ecco fatto, rimediato. E thx per la precisazione.

A proposito di Sniffing

Vorrei fare una precisazione su quanto detto nell'articolo "Sniffiamo gli indirizzi IP nelle chat", apparso sul numero 59. Viene detto che l'indirizzo IP è cifrato, ma non è del tutto vero: nei computer gli indirizzi IP espressi nella forma canonica xxx.xxx.xxx.xxx vengono sempre trasformati in un formato puramente numerico, per agevolarne la manipolazione. Se infatti guardiamo il campo che contiene l'indirizzo IP in una struttura iphdr noteremo che è espresso in termini di numero (u16) e non di stringa.
È quindi indifferente per il computer esprimere un indirizzo IP in entrambe le forme: verifichiamolo usando il comando ping! È corretto il metodo presentato per effettuare la trasformazione. Un saluto a tutti!

DktrKranz

Grazie, DktrKranz. Un contributo corretto e scritto nel modo migliore.

In attesa di WiMax

Posti per la Telecom sperduti, dove l'ADSL rimane solo un miraggio, ce ne sono tanti. Una connessione satellitare a internet unita a una connessione wireless che espanda il segnale in un raggio di un km sarebbe utile a molti. Qualcuno sa spiegare come si fa?

Figliocci

Si aspetta WiMax, www.wimaxforum.org, ovvero lo standard 802.16 che è un WiFi con velocità di trasmissione fino a 70 Mbit/secondo e su una distanza massima tra stazione base e terminale di 50 chilometri. Dovrebbe arrivare sul mercato nel 2005. Oppure ci si dota di parabola.
Una proposta un po' limitata è quella di www.tiscali.it, cercando Tiscali satellitare, oppure... guarda tra le altre risposte ai lettori.

SERVICE PACK 2

In merito all'articolo sul numero 59 "Sarà Service? OCCHIO al Pack!", vi posso assicurare che non è necessario avere la stringa 640 nel PID; ve lo dico per esperienza diretta ;-)

Simone

Confermiamo, e ti ringraziamo di averci scritto.

Che domande!

Come posso fare per diventare il più in fretta possibile hacker e senza farmi beccare? Volevo chiedervi anche se per favore potreste pubblicare un articolo nel quale spiegate come creare le crack e i keygen, magari con Turbo Pascal.

CoolHack

Sai cosa stona? Il "senza farmi beccare" e "il più in fretta possibile". Cosa pensi che sia un hacker? Hacker vuole dire essere aperti alla conoscenza, approfondire per sapere, curiosità, esplorazione... non è cercare di fregare qualcosa agli altri. Tanto meno è il "tutto e subito". Una vita, ci vuole, e non sarà abbastanza per capire tutto. Un consiglio: vai avanti a leggere HJ! Quanto ai crack, sai che non rispondiamo a domande del genere. Tutto si può fare, ma si deve anche saper scegliere da che parte stare.

Chi può rispondere?

Vi scrivo perché ormai siete rimasti la mia unica speranza. Volevo essere d'aiuto e riceverne... Quindi do una dritta chiunque abbia avuto dei problemi con la password della mmc su un nokia 6600.. Trovate la password in chiaro entrando in c\system e nel file mmcstore. Utilizzate programmi come Fexplorer o simili ke permettono di esplorare il sistema. Se il file manca (cm nel mio caso)...Boh..Chi mi aiuta?

Andrea

Giriamo ai lettori. Chi lo aiuta?

AES-128 a prova di bomba

Salve sono un vostro affezionato lettore sin dal primo numero. Vorrei porvi una domanda:tempo fa ho crittato un file .rar con lo standard AES-128, ma purtroppo ora non ricordo più la password,era un documento piuttosto importante e se sareste così gentili da aiutarmi ve ne sarei infinitamente grato.

Michele

Non è possibile. Sia perché non aiutiamo a realizzare un crack, sia perché AES-128 risulta indistruttibile.

Software biometrico

Volevo chiedervi se potete segnalami dove poter scaricare software biometrico. E magari software free. Volevo comunque far notare alla redazione che sarebbe auspicabile che la rivista fosse presente anche la rubrica di progettazione hardware di interfacce per i vari software in modo che possiamo interagire anche con l'esterno. Saluti.

cavin

Un programma gratuito di riconoscimento facciale, che funziona benino ed è anche molto divertente, lo troviamo qui: www.alparysoft.com/prod/videolock/index.php. È sufficiente una webcam e addestrarlo per riconoscere la nostra faccia. Esiste in versione freeware. Quanto all'hardware, cerchiamo di dare soluzioni non convenzionali. Ne vedrai.

Verità, innanzitutto

Scusate ma proprio ve lo devo scrivere! Maybe nessuno leggerà o nessuno risponderà ma io ve lo devo proprio di cuore! Su HJ 46 c'è un articolo a titolo "Autodistruzione" firmato da Barg the Gnoll dove si parla di un Galile0 che avrebbe aperto il suo disco rigido e ci avrebbe messo dentro, o sopra, un foglietto di carta vetrata! Mah io non è che sappia tutto, anzi..., ma mi sembra proprio grossa, questa, e non me la bevo! Mi sembra che un HD sia sottovuoto, o no? E poi come fa Galile0 a "dare un colpo" alla macchina e far cadere la carta vetrata sul disco? Ma dai, io dico che è una grossa panzana! Peccato, credevo che gli Gnolls (e anke HJ) dicessero sempre la verità! Un tanto per dovere! Ciao con cyberaffetto.

zooloo

A dire il vero un disco rigido dentro non è sottovuoto. Pensa, ad esempio, come fa la testina a stare sospesa a meno di un capello dalla superficie del disco, se non ci fossero effetti aerodinamici?
Se Galile0 avesse avuto la buona idea di fotografare il suo lavoretto prima di richiudere tutto, lo avremmo mostrato. È che i dischi rigidi non si aprono tutti i giorni ;-)

A volte possiamo sbagliarci e capita. Ma bugie, proprio no. Mai. La prossima volta che ti si rompe un disco, aprilo. C'è molto da imparare.

Barg the Gnoll
gnoll@hackerjournal.it

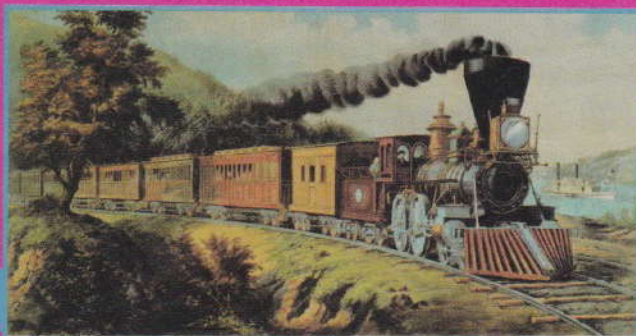
CARTE DI CREDITO e piccoli dettagli

Meccanismi e situazioni da conoscere per sapere tutto di come funzionano quelle piccole tesserine di plastica ed evitare i problemi

Ci siamo mai chiesti perché il Bancomat funziona digitando il codice segreto (il PIN) e invece la carta di credito no, basta la firma? La risposta è che soltanto la società che ha emesso la carta di credito può effettuare un controllo efficace sul PIN. I negozianti possono effettuare solo controlli parziali. Ecco perché nell'uso delle carte non ha mai preso piede il PIN. Di suo, tuttavia, sarebbe un sistema valido. Difatti, se proviamo a prelevare denaro usando la carta di credito, ecco che arriva la richiesta del PIN. Non tutti lo sanno, ma anche le carte di credito ne hanno uno.

Altra domanda: quando prenotiamo un albergo e ci viene chiesta la carta di credito, perché quel giorno possono esserci problemi con il limite di spesa e dal secondo giorno in poi invece tutto torna normale?

Prenotare e restare "senza soldi"

È capitato a molti, specialmente in

AMERICAN EXPRESS TRAIN

American Express è la carta ideale del Grande Fratello

vacanza, specialmente negli USA. Si prenota un bell'hotel per qualche giorno e succede esattamente quanto descritto. Ecco la spiegazione: come già sappiamo, tipicamente una carta di credito ordinaria ha un limite di spesa. Un'autorizzazione di spesa di solito genera un hold, una specie di prelazione, sulla somma in gioco. In pratica blocca quella cifra (anche se non c'è alcun addebito, i soldi restano sul nostro conto). Appena prenotiamo l'albergo per una settimana, viene bloccato l'importo equivalente, che può anche essere elevato. Andiamo poi a mangiare una pizza e in quella situazione il modesto importo della cena può comunque creare un problema.

Il giorno dopo, invece, sulla carta è stato effettivamente addebitata la prima notte; molto meno dell'intera cifra, che intanto è stata liberata e messa nuovamente a nostra disposizione.

In negozio invece funziona diversamente. Se stiamo concludendo un acquisto molto consistente, nel chiedere l'autorizzazione il negoziante potrebbe sentirsi rispondere dalla società emettitrice che occorre un controllo supplementare. In certi casi può accadere perfino che avvenga una telefonata a voce. Quando prevale il buon senso (o l'ingegneria sociale!), il limite può essere aggirato limitatamente alla singola transazione.

Il limite non basta mai

C'è gente che fa la carta di credito apposta per andare in vacanza. Partono e si accorgono praticamente subito che la carta ha un limite e che quel limite è basso. Sul conto ci sono soldi a palate, ma è impossibile spenderli. Soluzione: telefonare alla società emettitrice e chiedere di alzare il limite.

Per mestiere, chi risponde farà del suo meglio per impedire che ciò avvenga. Dirà che bisogna mandare un fax piuttosto che una raccomandata, che ci vogliono quindici giorni, che occorre una autorizzazione della banca e altre storie. Non è vero niente. Possono farlo e possono farlo subito senza dover ricevere alcun fax. Il modo per farsi alzare il limite della carta è insistere, gentilmente ma con fermezza.
C'è chi si inventa situazioni di emergenza (siamo all'estero, si è rotta la macchina, dobbiamo noleggiarne un'altra, c'è stato un incidente eccetera). C'è persino chi telefona da casa propria, raccontando di essere all'estero e di avere necessità!

AMERICAN EXPRESS TI GUARDA

Le carte di credito di solito hanno un limite, ma American Express (AMEX) si comporta in modo diverso. AMEX è la carta ideale del Grande Fratello (quello di Orwell, non quello di Aran Endemol): approva le transazioni in funzione degli utilizzi passati, dello storico dei pagamenti e dei dati finanziari del titolare della carta. Sempre AMEX, inoltre, per convenzione non farà mai dire "no" a un cliente da una macchina. Se il meccanismo di autorizzazione elettronico ritiene che la transazione sia rischiosa chiederà al negoziante di sentire direttamente la società di emissione e magari vorrà parlare anche con il titolare della carta. Quest'ultimo si sentirà chiedere informazioni, mai le stesse due volte, di carattere personale e anche finanziario. Chi tiene molto alla propria privacy personale fa bene a pensarci due volte prima di attivare una carta American Express.

AMERICAN EXPRESS

PER UNA CARTA DI CREDITO SICURA

1) firmarla subito appena arriva e non lasciarla in bianco (è vero che se non è firmata ci chiedono un documento, ma se ce la rubano, la firmano e la usano liberamente);
2) trasportare la carta in un luogo diverso dal portafogli;
3) tenere nota dei dati della carta in un posto sicuro e mai insieme alla carta;
4) tenere sempre d'occhio la carta durante una transazione e recuperarla appena possibile;
5) conservare gli scontrini in luogo sicuro o distruggerli. Mai buttarli via!
6) tenere d'occhio gli estratti conto e confrontarli con gli scontrini o con una nostra nota delle spese fatte;
7) preavvisare in anticipo la società emittente di un cambio di residenza;
8) mai, mai, mai prestare la carta a chicchessia;
9) mai firmare una ricevuta in bianco. Barrare tutti gli spazi vuoti sulla ricevuta;
10) mai comunicare a entità non fidate i dati della carta.

RICATTO

Casino al casinò

Che fare quando una banda di pirati di chissà dove prende in ostaggio il tuo sito? A qualcuno è successo e non tutti se la sono cavata in maniera indolore...

▲ *Dopo gli attacchi ai casinò online non sono solo i giocatori a restare in mutande!*

A luglio li hanno presi. Una banda russa metteva fuori combattimento i server delle agenzie inglesi per le scommesse, mediante attacchi DDoS, e poi chiedeva soldi per non farlo più.

La National Hi-Tech Crime Unit britannica ha collaborato con le autorità russe fino quando non sono stati rintracciati i tre colpevoli. Tra i 21 e i 24 anni, Chiedevano somme di dieci-ventimila dollari, con punte di 55 mila. Ma ci è voluto tempo e, dall'ottobre 2003 in cui è partita la denuncia, i pirati sono riusciti a fare danni per importi di centinaia di migliaia di euro se non di più. Alla fine si è scoperto pure che gli stessi avevano cercato di ricattare gli scommettitori statunitensi nell'imminenza del Super Bowl, la finalissima del football americano.

Non è sempre luglio

Ma ad altri invece è andata molto meno bene. Parliamo di Multibet (http://www.multibet.com), società di scommesse che fa capo all'australiano Terry Lills, operante in una decina di nazioni.

I ricattatori si fanno vivi e chiedono a Lills più di 15 mila euro in cambio di protezione. Lui li manda a quel paese e loro, cinque minuti dopo, gli bloccano il sito con un attacco DDoS: una mazzata che blocca il business per quasi tre settimane provocando danni incalcolabili.

CHE COS'È UN DDOS

DDosS sta per Distributed Denial of Service. Attacco in cui una moltitudine di sistemi compromessi (per questo si chiama distribuito) bombarda suo malgrado un bersaglio, che crolla sotto un numero di pacchetti eccessivo per le sue capacità e non può più svolgere le proprie funzioni.

Alla fine Lills capitola e paga. Adesso lavora, ma ogni mese versa un pizzo su un conto lituano attraverso un pagamento Western Union.

Intanto la polizia australiana è sulle tracce dei malviventi, in collaborazione con svariate forze dell'ordine europee. Quando li troveranno è probabile che sarà un bel botto, perché per bloccare tre settimane un sito bisogna avere un bell'esercito di zombi.

Computer ignari e dormienti

Gli zombi sono, in gergo, i computer che servono per l'attacco. Sono migliaia, posseduti per lo più da cittadini ignari oppure aziende con pessimi amministratori di rete. Il ricattatore ne prende possesso con un worm e, quando serve, fa scatenare l'attacco. Secondo certe stime, l'uno per cento dei computer su Internet potrebbe essere compromesso. Forse il nostro computer viene usato in questo esatto istante per scatenare un attacco, insieme ad altri mille o diecimila. Diecimila zombi sono un patrimonio, che vale al suo padrone anche qualche migliaio di euro.

La nuova frontiera del ricatto informatico sono ora i casinò online. Fanno un sacco di soldi, dipendono completamente dal web, i proprietari li aprono in paradisi fiscali dove non si pagano tasse ma è ben difficile ottenere collaborazione dalla polizia.

Nel complesso, in questo momento l'eterno gioco di guardie e ladri è a favore di questi ultimi. Speriamo che la tendenza si inverta, prima di ritrovarci alle prese con bande di estorsori da due soldi che minacciano i siti della gente comune.

NON SOLO ROMERO

Per zombi si intende un computer infettato con un worm o un trojan, sfruttabile da remoto per lanciare attacchi DDoS all'insaputa del proprietario.

NHTCU E POLIZIA POSTALE

In Inghilterra la National Hi-Tech Crime Unit (http://www.nhtcu.org/) è nata nel 2001, quando il governo britannico ha preso atto di un rapporto che denunciava gli alti rischi dovuti all'attività dei criminali informatici. Da noi invece vigila sul cibercrimine la Polizia Postale Informatica, istituita nel 1998 e sempre più puntuale e precisa, dopo una partenza sinceramente goffa.
Si trova su http://www.poliziadistato.it/pds/informatica/index.htm, con consigli per la navigazione su Internet dei bambini (!) e qualche segnalazione di truffa in corso.

Denial Of Service: l'INPUT Imprevisto

Uno degli attacchi maggiormente utilizzato dagli script kiddies o dai lamer, per la sua semplicità di esecuzione, è senz'altro il DoS (denial of service : negazione del servizio), ovvero un attacco mirato a un momentaneo crash del sistema target o dell'applicazione presa di mira. I metodi con cui eseguire l'attacco sono tanti, uno di quelli maggiormente sfruttato è "l'input imprevisto". Vediamo come è possibile.

Lo strumento principale che abbiamo in mano è la conoscenza. Quindi capire come funzionano tutti i possibili attacchi ai nostri server è il primo passo per migliorarne la sicurezza

Il Web e le applicazioni

Inquadriamo quindi il problema nell'ottica di Internet. Pensiamo un attimo a un sito Web che propone un qualunque modulo HTML di registrazione, il quale deve dare la possibilità all'utente di scegliere solo tra le opzioni proposte.

Ecco un esempio:

```
<FORM ACTION="processadati.cgi"
METHOD="GET">

<SELECT NAME="scelta">
<OPTION VALUE="hj">H4ck3r Journal
<OPTION VALUE="hm">H4ck3r Magazine
<OPTION VALUE="prhack">Prh4ck
</SELECT>

</FROM>
```

Se scegliessimo, per esempio, la rivista Hacker Journal il browser provvederebbe

150 ARRESTI PER DDOS

Molti gli arresti di cracker americani che hanno scatenato diversi attacchi DDoS (distribuited denial of service), alcuni addirittura pagati da società che volevano far fuori telematicamente la concorrenza. Ma attualmente è la mafia lituana la principale accusata e la più pericolosa in questo utilizzo criminale della rete, ricattando grandi provider telematici i cui servizi sono abbattuti da massicci attacchi DDoS se non pagano un adeguato 'pizzo'.

a inviare il seguente URL:

"processadati.cgi?hj"

ma nessuno ci impedisce di inviare manualmente quest'altro URL:

"processadati.cgi?script%20kiddies".

Se l'applicazione che gestisce il modulo (in questo caso lo script cgi processadati) facesse affidamento sul fatto che apparentemente il modulo limita la scelta con il costrutto SELECT e non fosse programmata per gestire i dati superflui, potrebbe chiudersi con un bell'errore, impedendo così il corretto funzionamento del modulo per altri utenti.
I siti più grandi ovviamente prendono molte precauzioni per i moduli e per il programma che li gestisce, ma un sito più piccolo potrebbe essere esposto a questo attacco. È dunque necessario che facciamo sempre un filtraggio dei dati in input, anche se apparentemente questi sono limitati a delle opzioni proposte dal codice HTML.

Mascheramento

Un altro aspetto interessante, anche se non è definibile un vero attacco DoS, è quello del mascheramento degli URL tramite codifiche esadecimali o standard tipo UTF8/UNICODE, supportato da quasi tutti i server.

Se passiamo a un server la richiesta della directory /cgi-bin/ con il file di Unix phf tramite un URL di questo tipo:

http://dominio.com/cgi-bin/phf

generalmente il browser ci risponde con un cgi error o con un errore 403, in cui ci dice che non siamo autorizzati ad accedere alla directory richiesta.
Questo perché molti siti bloccano gli URL contenenti stringhe tipo /cgi-bin/ .
Ma se noi inviamo la richiesta in questo modo tramite Telnet:

/%63%67%69%2d%62%69%6e/phf

il server convertirà la stringa esadecimale in caratteri ASCII, provvedendo ad aprire la directory richiesta, in questo caso /cgi-bin/phf, ma la richiesta passata non è esattamente uguale a questa:

http://dominio.com/cgi-bin/phf.

Ammettendo ora che il server abbia Microsoft IIS su Windows NT e che noi volessimo aprire la shell dei comandi MS-DOS, potremmo passagli una richiesta del tipo:

/cgi-bin/..%c0% af..%c0%af..%c0%af..%c0afwinnt/system32/cmd.exe

che è una stringa codificata con i simboli di escape UTF8/UNICODE simile a

/cgi-bin/../../../../winnt/system32/cmd.exe

che risale il file system dall'unità root verso la cartella dove è presente la shell di MS-DOS, ovvero

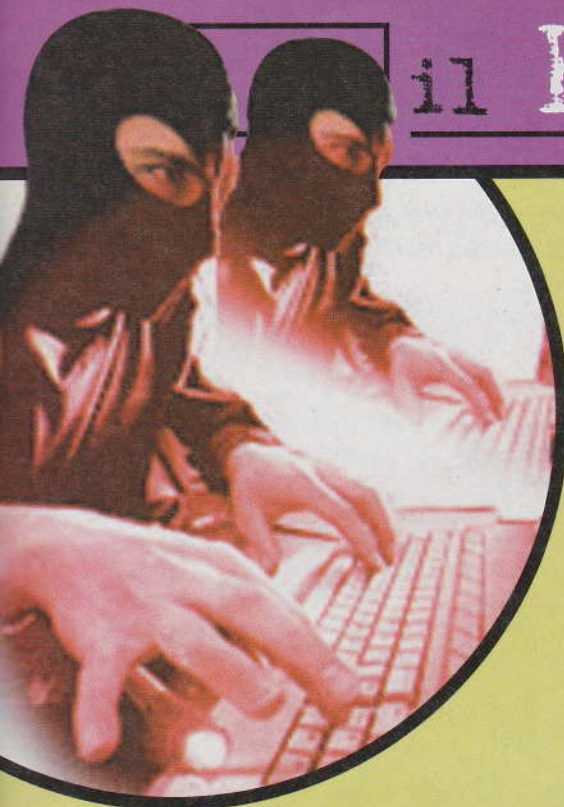
cmd.exe.

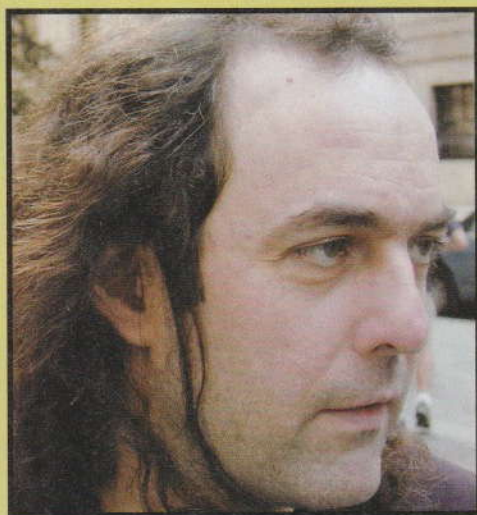
Cosa abbiamo imparato

L'attacco DoS è un attacco a cui molti siti possono essere vulnerabili e che porta alla disabilitazione momentanea del sito o di qualche sua applicazione, che diventa irraggiungibile agli altri utenti.
Se non prendiamo precauzioni di filtraggio sui moduli di immissione dati dei nostri siti, siamo estremamente vulnerabili ad attacchi di questo tipo.
Se non prendiamo provvedimenti, con tecniche simili e che prevedono l'immissione manuale di stringhe in formati diversi da ASCII, qualche malintenzionato potrebbe risalire facilmente alle directory contenenti i file di sistema del nostro server.

Lord Anonymous

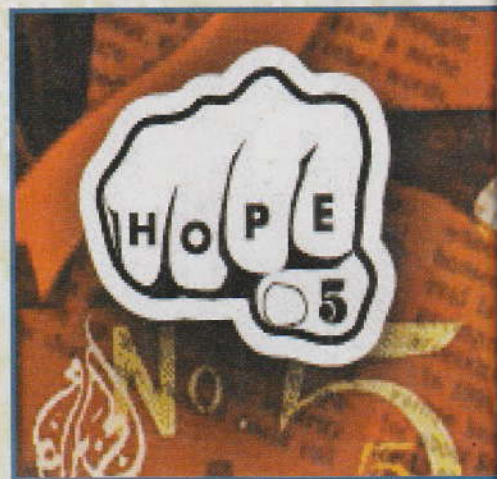
ALL'ATTACCO DEI LINK

Possiamo trovare un forum di discussione sugli argomenti qui brevemente presentati nel sito http://lordanonymous.altervista.org, con un topic in più: l'input imprevisto nelle query SQL.
Un altro sito con parecchi puntatori a documenti che riguardano l'argomento: www.denialinfo.com/

MR. 2600: EMMANUEL

La sua specializzazione: Hacker information. Ma se sentiamo un sibilo a 2600 hertz, sicuramente è lui!

New York City, 31 agosto 2004, vicino a Union Square stanno marciando rumorosi dimostranti contro la convention repubblicana. Sotto elezioni, si sa, può accadere di tutto e un'implacabile telecamera appesa allo spigolo con la 16esima strada registra l'arrivo della polizia. 150 dimostranti vengono caricati su piccole camionette e portati via. La manifestazione si scioglie tra le urla dei partecipanti in fuga. Pochi quotidiani al mondo ne hanno riportato notizia. Normale amministrazione, cose che succedono. Ma alla redazione di "2600 - the hacker quaterly", sono in subbuglio. Tra i variegati personaggi caricati dai poliziotti, anche il loro storico fondatore: Eric Corley, più conosciuto come Emmanuel Goldstein.
Le ultime notizie lo danno nuovamente libero dopo 32 ore di cella e di accertamenti.
Non dev'essere stato facile, dati i precedenti.

All'inizio degli anni novanta, infatti, sia la rivista, sia il suo fondatore, finirono nel mirino di un tribunale accusati dall'MPAA, la potente associazione per i diritti cinematografici americana, di "distribuzione di software illegale". L'accusa a Goldstein era quella di permettere la distribuzione di DeCSS, la famosa utility per la decodifica dei DVD. Convinto in una risoluzione positiva della causa, sarà costretto invece a crollare di fronte alla corte distrettuale di New York, appena dopo ferragosto del 2000. Goldstein dovette togliere il software dal proprio server e pagare le spese processuali.

Hacker teorico e letterato

Cresciuto a Long Island, New York, si appassiona immediatamente di tecnologia, ma ne è affascinato come davanti a una splendida ragazza nuda

HOPE, l'Hacker On

sul web: intoccabile. Vive d'hacking senza infilare le mani nella marmellata, lo teorizza senza sporcarsene. Ma è proprio così? Innamoratosi della radiofrequenza e inventatosi conduttore radiofonico, quando si iscrive alla State University of New York diventa il mattatore della radio del college. Parallelamente alla cultura hacker, in quegli anni si sviluppava e diffondeva con rilevante velocità la cultura yippie con elementi di spicco come Abie Hoffman. Proprio tale figura sarà un punto di riferimento importante per Goldstein.
Sempre più teorizzando che praticando (almeno all'apparenza), poco tempo dopo Emmanuel diventerà uno dei nomi più gettonati e rispettati nell'ambiente dell'hacking, per lo spirito propositivo, le numerose campagne pro-hacker e l'informazione continua in varie riviste con le quali collaborava.
Eric fonda la rivista hacker per eccellenza: "2600: The Hacker Quarterly". Specializzatosi in phreaking e ingegneria sociale, deriverà il nome della rivista dalla frequenza del tono emesso dai telefoni per le connessioni interurbane negli Stati Uniti: 2.600 hertz.

GOLDSTEIN

Planet Earth...

Un gruppo di 60 mila

La rivista s'impone subito beccandosi una bella fetta di mercato underground: circa sessantamila fidati lettori sparsi in tutto il mondo. Così si candida automaticamente come quella più autorevole fra gli hacker e quella maggiormente sorvegliata da parte delle autorità e dei tribunali americani.
Anche perché, dopo la fondazione, 2600 segue da vicino le vicende più importanti di hacking e lancia pesanti campagne contro le autorità. Appena può, Goldstein si lancia in accuse contro le sentenze emesse dai tribunali, che ritiene ingiuste ed esagerate. Un ribelle a tutti i costi? Forse, ma non è che avesse sempre tutti i torti. Come nel caso di Craig Neidorf, conosciuto come Knight Lightning. Il ragazzo s'era dato da fare ed era riuscito a entrare nei sistemi della Bell South, aspirandone fuori un bel pacco di quelli che erano considerati segreti industriali.
Siccome quest'hobby, si capisce, non è particolarmente gradito a chi su quei segreti ha investito milioni di dollari, venne arrestato e processato duramente. Che fine ha fatto? È stato assolto, che ci crediamo o no, perché la rivista 2600 dimostrò come il materiale che Knight Lightning aveva sottratto dai sistemi Bell South poteva regolarmente e legalmente essere comprato per pochi dollari. Forse Knight non se l'era procurato così, ma questa è un'altra storia.

Le ultime lotte

Agosto 1994: 2600 invita tutti quanti seguono la rivista a partecipare alla prima conferenza planetaria degli hacker, HOPE. Durante l'Hacker On Planet Earth si parla di tutti gli aspetti dell'hacking, delle ultime vicende in ambito giudiziario, c'è la presentazione di nuovi software, si accendono discussioni tecniche, ma soprattutto si parla del Condor. Kevin Mitnick è in prigione e l'HOPE lancerà il primo grido di "liberiamo Kevin". Nel 2000, il 21 gennaio, Eric Corley si reca davanti al carcere dove pochi minuti dopo viene rilasciato finalmente il Condor. Goldstein non resiste al microfono e, in diretta su "Off the Hook", una trasmissione divenuta famosa e trasmessa dalla stazione radio WBAI, parla e fa parlare il suo ospite d'eccezione, che negli anni di galera ha potuto certamente meditare un bel discorso.

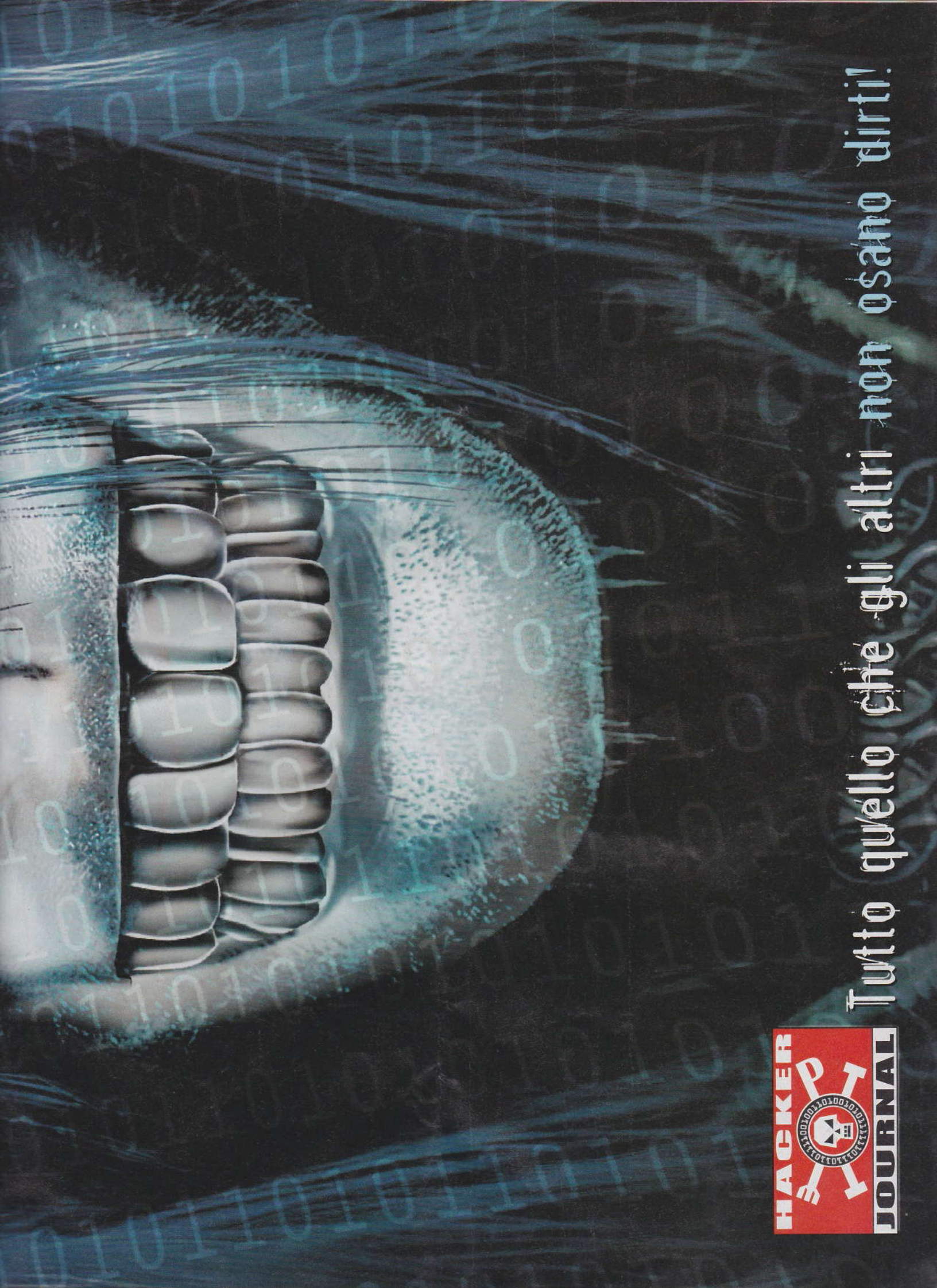
Gli anni passano per tutti, però. Lo spirito battagliero di alcuni si affievolisce e, salvo qualche battaglia vissuta ancora sul campo, oggi queste rimangono figure di un mondo cambiato. Ce l'ha dimostrato un Mitnick tutto giacca e cravatta, consulente per la sicurezza, che alla quinta conferenza HOPE si è esibito con Goldstein in uno straordinario show dialettico.

Con il contributo di: Alone Sparrow

Orwell 1984

Goldstein non è altro che il nome che George Orwell diede al protagonista di "1984", la figura ribelle, colui che scrisse "The Book", Il Libro, che comprendeva tutte le eresie, che veniva fatto circolare clandestinamente un po' dappertutto. Oggi c'è addirittura chi paragona la figura originaria di Goldstein come quella del diavolo, o di Bin-Laden. La discussione è ancora aperta...

L'autore di 1984, il creatore del Grande Fratello.

Una delle prime copertine della mitica rivista 2600

HACKER
JOURNAL
Tutto quello che gli altri non osano dirti!

Dalla TEORIA al

Che cosa serve per fare con successo Voice over IP e parlare su Internet come se fosse una linea telefonica

Abbiamo già parlato alcuni numeri orsono dell'hardware minimo per fare Voice over IP e fare viaggiare la voce su Internet: un PC con processore 386, una scheda audio full duplex e naturalmente un collegamento a Internet. Sono requisiti ampiamente superati da qualsiasi computer che abbia meno di cinque anni. A questi va aggiunta talvolta una scheda di accelerazione hardware come PhoneJack o LineJack di Quicknet (http://www.quicknet.net/), in grado di comprimere l'audio con grande efficienza. Ma ora parliamo un po' di software.

Il sistema operativo

Non ci sono problemi nello scegliere Windows, Mac OS X oppure Linux: vanno tutti e tre benissimo. Al massimo ci saranno scelte diverse.

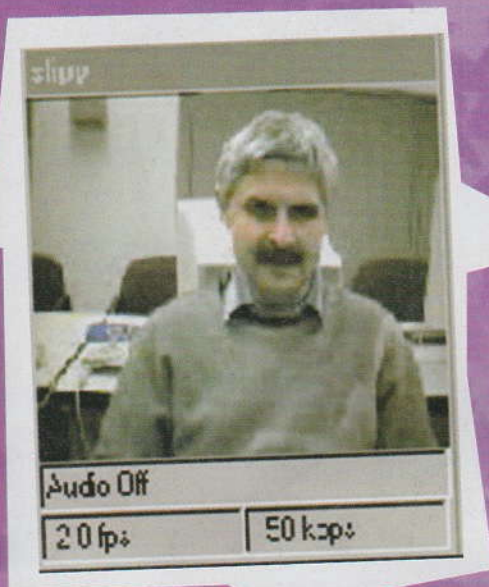
Sotto Windows i software che fanno VoIP sono numerosi: solo per citarne qualcuno, Netmeeting, Internet Phone, DialPad. Chi usa schede Quicknet potrebbe anche optare per Internet Switchboard. E naturalmente c'è tutto il software libero reperibile grazie al lavoro del gruppo OpenH323 (http://www.openh323.org/).

OpenH323 è la scelta obbligata su Linux. Alcuni programmi della gamma, come simph323 oppure ohphone, funzionano anche con le schede di accelerazione hardware Quicknet.

Su Mac OS X, Apple offre iChat AV

Su http://www.cisconetwork.net/ html/index.php si trova questo telefono Cisco, che fa Voice over IP e lo fa anche wireless!

PROGRAMMI CHE USANO H.323

Microsoft NetMeeting - http://www.microsoft.com/windows/netmeeting/
Net2Phone - http://www.net2phone.com/
DialPad - http://www.dialpad.com/
Software open source (per esempio GnomeMeeting e Ohphone nell'ambito del progetto OpenH323 - http://www.openh323.org/

(http://www.apple.com/it/ichat) e poi si può usare tutto il software che esiste per Linux. A volte è già pronto (riferirsi a http://xmeeting.sourceforge.net/ o http://www.ioxperts.com/apps_osXvideo.html), a volte va ricompilato.

Software di gateway

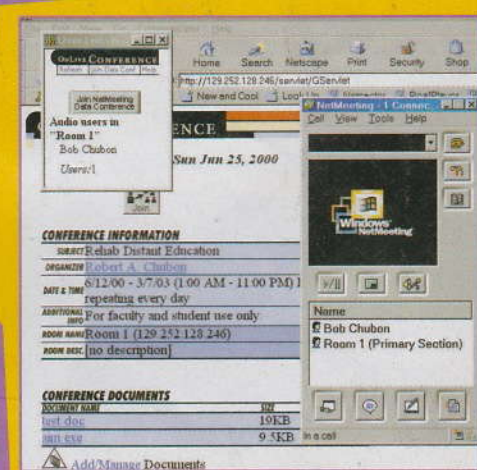
Supponiamo di voler fare VoIP e arrivare, quando necessario, su linee telefoniche tradizionali (PSTN, Plain Standard Telephone Network). In questo caso serve software di gateway, come Internet SwitchBoard (http://www.quicknet.net/) per Windows, oppure PSTNGw, reperibile nel software OpenH323, che funziona su Windows ma anche su Linux. Servirà anche software di gatekeeper, ossia di gestione di tutto l'apparato. OpenH323 mette a disposizione GNU Gatekeeper, a http://www.gnugk.org/, e Opengatekeeper, per Linux e Windows.

Un ultimo software utile per risolvere problemi è Phonepatch (http://www.equival.com/phonepatch), che sa aggirare problemi generati dalla presenza di firewall NAT. Phonepatch consente agli utenti (dentro o fuori dal firewall) di chiamare da una pagina web. Quando la web application presente sulla pagina capisce che il destinatario della chiamata è pronto, avvisa il chiamante e a quel punto si può stabilire la comunicazione. Phonepatch, al contrario di molto software presentato qui, è proprietario, ma si può scaricarne una versione demo che consente conversazioni lunghe fino a tre minuti.

APPROFONDIAMO

http://www.openh323.org/standards.html la documentazione integrale sugli standard che formano H.323

http://www.cs.columbia.edu/~hgs/rtp/h323.html sempre la documentazione ma anche esempi e guide rapide

http://www.itu.int/itudoc/itu-t/rec/h/ tutti gli standard della serie H, presso il sito ITU

▲ *Oltre a essere una gran comodità, poter usare la voce su Internet è di aiuto anche per i disabili.*

TRUCCHI e SEGRETI di Windows

Windows non finirà mai di stupire e di darci tante possibilità di esercitare la nostra voglia di hacking

Segreto numero uno: negativo!

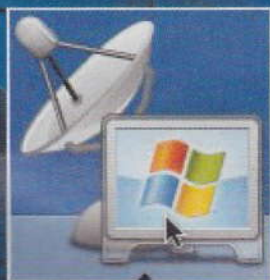
Diciamo che abbiamo appena acquistato un nuovo pc e, siccome siamo bravi e non vogliamo perdere nulla dei nostri lavori passati, abbiamo trasferito tutte le cartelle del vecchio pc al nuovo. Compresa una cartella con il nome desktop, che abbiamo riempito per comodità con le cose che avevamo proprio su desktop del vecchio computer. La sistemiamo per bene sulla scrivania del nuovo pc, così da averla sott'occhio. Peccato che:

- **se con un clic cerchiamo di aprire un nodo delle directory,** ovvero facciamo clic sul simbolo (+) che indica che sotto alla cartella ci sono altri oggetti, la cartellina potrebbe non aprirsi più;
- **la cartella Desktop (quella vera, del nuovo computer),** potrebbe venire replicata parecchie volte;
- **a tutte le altre cartelle, o a qualche cartella caso,** potrebbe venire cambiato il nome con caratteri spuri e casuali;
- **noi ci troveremmo davanti agli occhi una serie di messaggi più o meno di questo tenore:**

"F:\Documents and Settings\Amministratore\Desktop\Desktop\Desktop si riferisce a una locazione non disponibile. Potrebbe essere su un disco rigido di questo computer o su una rete. Verificare che il disco sia inserito o che siate col-

legati a Internet o alla rete, e provare di nuovo. Se comunque non si trova, l'informazione potrebbe essere stata spostata su una locazione differente"

Tutti errori che possono comparire assieme, uno alla volta o non comparire affatto, per un po'. Cosa succede? Semplice: dobbiamo assolutamente evitare di creare una cartella di nome Desktop sul Desktop, pena la demenza precoce di esplora risorse. Parola di tanti utenti che si sono trovati in situazioni al limite dell'assurdo e parola di Microsoft, che ci avverte con la nota tecnica leggibile all'indirizzo: http://support.microsoft.com/default.aspx?scid=kb;en-us;323681&Product=winxp#appliesto

Trucco numero due: positivo

Quando lavoriamo con il Desktop Remoto, possiamo dare al computer remoto il comando di spegnimento. È sufficiente che apriamo il Blocco Note, o qualcosa di analogo, e scriviamo questa linea di istruzioni:

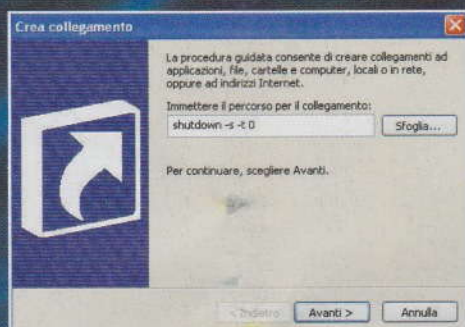
```
(newActiveXObject("Shell.Application")).ShutdownWindows();
```

Quindi salviamo il file sulla scrivania chiamandolo RemoteShutdown.js. Un doppio clic attiva lo spegnimento del pc.

Trucco numero tre: positivo!

Buttiamo via tutto quello che possiamo! Ne guadagneremo in spazio su disco e velocità di funzionamento. Una cartella da svuotare senza pietà in Windows XP è C:\Windows\Prefetch. Una bella ripulita non fa assolutamente nulla di male e i file che servono vengono ricreati automaticamente di nuovo, fino al successivo svuotamento.

Trucco numero quattro: positivo

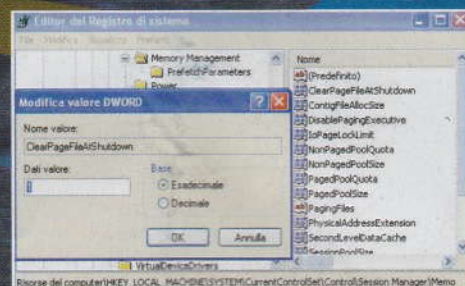
Spegnere velocemente il pc con Windows XP? Facile, basta che seguiamo questi passi:

- clic destro su un punto qualunque della scrivania, Nuovo > Collegamento
- nel percorso scriviamo:

```
shutdown -s -t 0
```

(per non sbagliarsi lo diciamo in chiaro: shutdown[spazio]-s[spazio]-t[spazio]cifra zero).

- un clic su Avanti e chiamiamolo Spegnimento, o come vogliamo.
- due clic sull'icona creata sulla scrivania e il pc va a nanna.

Segreto numero cinque: positivo

Nei file di paging di Windows sono appoggiate, come una cache, le informazioni che sono riallocate dalla Ram, quando questa non basta o serve altro spazio. Windows è predisposto a lasciare inalterato questo file anche quando si spegne il pc. Ma noi possiamo attivare la cancellazione del file di paging tutte le volte che lo spegniamo. L'unico problema è che aumenta il tempo di spegnimento. Basta saperlo.

Entrare in regedit tramite Start > Esegui > regedit
Cercare la stringa

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

Selezionare

```
ClearPageFileAtShutdown
```

dalla lista sulla destra e con un clic destro selezionare Modifica. Cambiare il valore a 1 e clic su Ok. Riavviare il pc.

Segreto numero sei: negativo

Supponiamo di dimenticare la password di ingresso in Windows XP. Possiamo creare un disco di ripristino della password che ci darà la possibilità di ricostruirla. Peccato che se ci dimentichiamo in giro il disco, chiunque potrà cambiare la password del nostro account.

Andiamo su Start/Impostazioni/Pannello di Controllo/Account Utente e un clic sull'account di cui vogliamo

creare il disco di ripristino. Un clic su Reimpostazione Password attiva la Creazione guidata disco di reimpostazione password. Inseriamo un floppy vuoto e proseguiamo. Per usare il floppy di ripristino invece di inserire la password, un clic sul punto di domanda e sulla scelta del disco di ripristino. Seguendo la reimpostazione guidata della password se ne potrà inserire una nuova.

Come OSI parlarmi così?

Come fanno computer tanto diversi a capirsi tra di loro? OSIamo una spiegazione, che userà termini come "Livello fisico" o "Livello di trasporto". Capirli, ci porterà un po' più in là

Trovarsi su un campo di calcio non significa poter giocare a calcio. È necessario che tutte e due le squadre conoscano le regole, sappiano come iniziare il gioco, nominino un arbitro per sedare le risse... La stessa cosa vale per i nostri computer. Avere la scheda di rete non vuole dire che se li colleghiamo uno con l'altro, questi riescano a parlarsi. Tantomeno se stanno usando sistemi operativi o applicazioni differenti. Bisogna che tutti e due rispettino le stesse regole.

Gli arbitri internazionali, ovvero l'organizzazione di standardizzazione ISO, hanno cercato allora di mettere d'accordo tutti quanti creando un insieme di regole, ovvero un modello, chiamandolo Open System Interconnection: OSI, appunto.

Il modello nudo

OSI è fatto di sette strati, ciascuno dei quali ha una sua specifica funzione e parla con il livello che gli sta sopra e con quello che gli sta sotto. Più ci si abbassa di livello e più la comunicazione diventa primitiva. Il primo livello è quello fisico, dei cavi o dei mezzi di trasporto usati per trasferire i dati. Il livello più nobile, quello al settimo piano, è invece tutto dedicato a chiacchierare con le applicazioni che stiamo usando.
In mezzo, ci sta per esempio la cifratura e tutte le altre belle cose che vogliamo fare. Il concetto di base è quello che ciascun livello fa cose che non richiedono cambiamenti nei livelli sopra e sotto. Spezzando così il problema della comunicazione tra due computer, lo si fa diventare più facilmente maneggiabile. Basta influire sul livello giusto e solo su quello, e il gioco è fatto.
È un po' come dire, per esempio, che possiamo inviare la posta elettronica sia su cavo adsl che su fibra ottica o attraverso il modem, senza dover cambiare programma.

Vedendolo, è meglio

Guardiamo in pratica cosa succede.

OSI CONTRO TCP

Dove stanno i protocolli come il TCP (transmit control protocol) e l'IP (internet protocol) nel palazzo dei sette piani OSI?

In questo schema vediamo le corrispondenze. Gli attacchi DoS a base di ping, per esempio, riguardano il livello tre (leggiamo l'articolo D.o.S. Parte 1a - PING DELLA MORTE, aprile 2003, www.hackerjournal.it). Gli exploit che invece riguardano il TCP, li collochiamo a livello quattro.

HACKER JOURNAL

▲ *La trasmissione inizia al livello 7. Dobbiamo spedire il messaggio "Hacker Journal", tramite un'applicazione qualunque, per esempio di posta elettronica.*

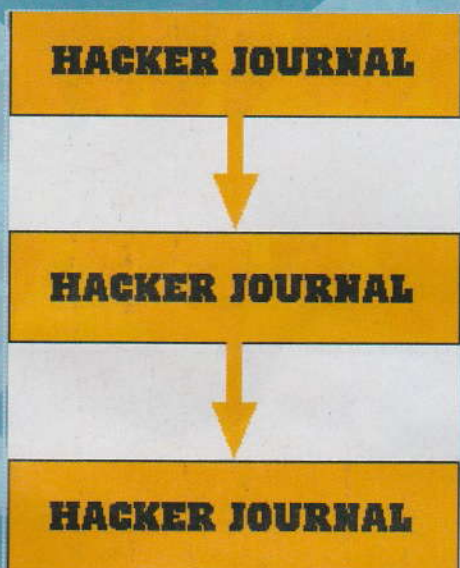
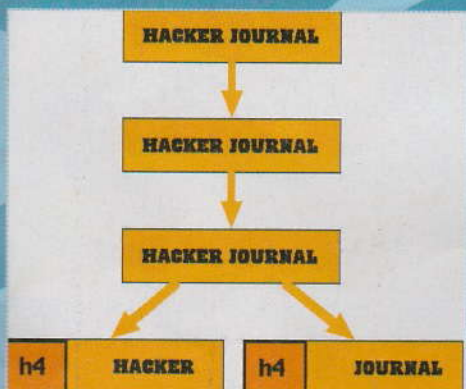
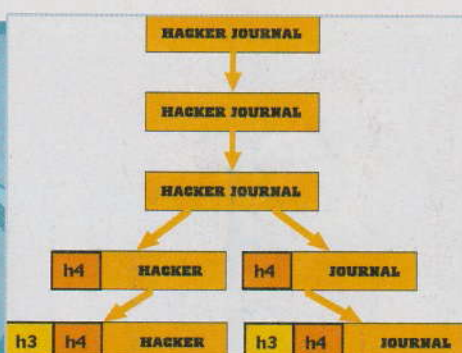
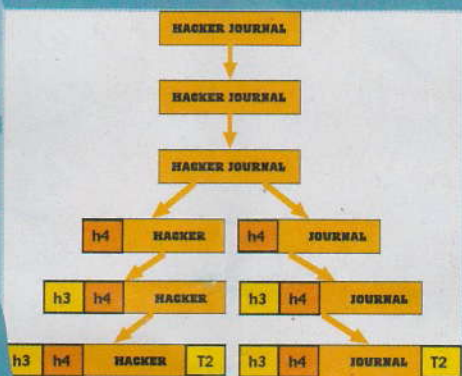
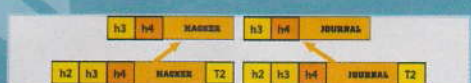
HACKER JOURNAL

HACKER JOURNAL

▲ Il messaggio viene preparato dal livello 6 per essere accettato dai livelli più bassi. Compressione o cifratura si collocano qui.

HACKER JOURNAL

HACKER JOURNAL

HACKER JOURNAL

▲ Praticamente nessun cambiamento significativo. A questo livello, il 5, viene soprattutto regolato il flusso di dati.

▲ Siamo sempre dentro il computer che sta trasmettendo. A livello 4 il dato è spezzato in pacchetti più semplici e viene attaccata un'intestazione a ciascun pacchetto. Le intestazioni comprendono numeri sequenziali e altre informazioni di controllo.

▲ Livello 3: ci stiamo velocemente avvicinando alla vera trasmissione dei pacchetti. Qui viene aggiunta un'altra intestazione, che servirà al pacchetto per essere instradato sul percorso per la destinazione.

▲ Siamo pronti, viene agganciata una coda per adeguare i pacchetti al sistema che trasporterà effettivamente i dati. Sotto questo livello, i pacchetti saranno già su qualche mezzo fisico che li dovrà trasportare, sia esso la microonda di un dispositivo WiFi o il cavo della rete Ethernet.

▲ Il messaggio raggiunge un computer sulla rete a cui siamo collegati. Tale computer controlla che il messaggio sia per lui. Non lo è, quindi passa il messaggio al livello 2.

h3 h4 HACKER h3 h4 JOURNAL

h2 h3 h4 HACKER T2 h2 h3 h4 JOURNAL T2

▲ Il livello 2 lo rispedisce al livello fisico per fargli proseguire la corsa verso la macchina di destinazione.

h2 h3 h4 HACKER T2 h2 h3 h4 JOURNAL T2

▲ Finalmente abbiamo ricevuto il pacchetto. Sono eliminate la prima intestazione e la coda. Il pacchetto pulito e pronto per essere passato al livello 3, di Rete.

▲ Si controlla che il pacchetto sia veramente per questo computer e lo si passa al livello 4, il livello di Trasporto.

▲ Prima di passarlo al livello 5, è scartata l'intestazione. I pacchetti che formavano assieme il messaggio completo sono preparati per essere rimessi assieme.

▲ Ricomposto al livello 5, il nostro messaggio è decifrato, decompresso, riformattato a dovere per assumere l'aspetto originale. Le intestazioni e le code sono state rimosse e l'applicazione che lo riceve può metterlo in chiaro. Dopo una bella faticaccia, la nostra email è arrivata, in questa rete che utilizza lo standard ISO/OSI.

433 esempi in 132

FACCIAMO QUADRATO

Curiosiamo dentro ogni singolo esempio dei linguaggi descritti per intuire subito un sacco di cose e farci le ossa per la programmazione. Ecco, per esempio, il calcolo del quadrato di un numero tra 1 e 10 con il linguaggio Oz/Mozart, funzionale:

```
local ShowIt T in
  proc {ShowIt T}
    {Show T*T}
  end
  {For 1 10 1 ShowIt}
end
```

ed eccolo in C#, procedurale

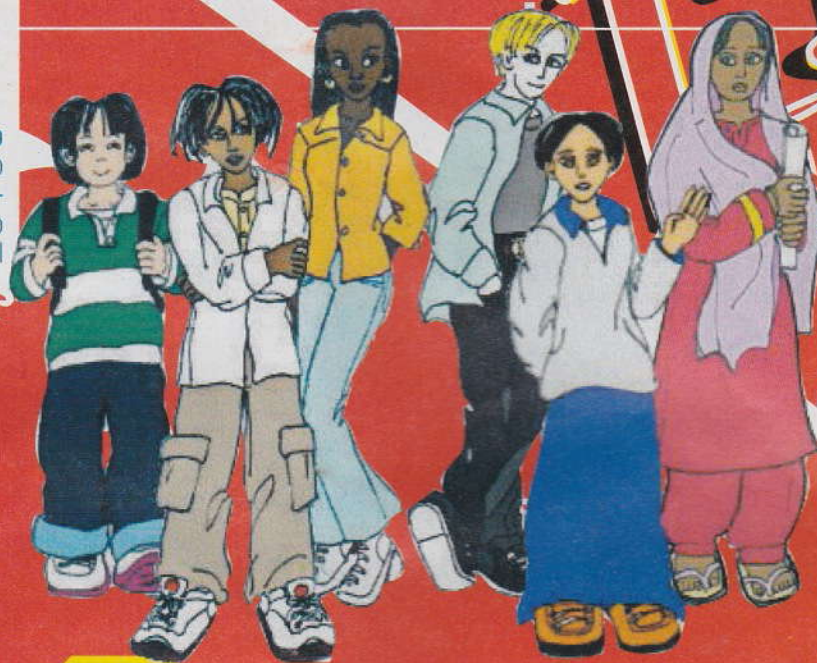
```
using System;
class Squares1 {
  static void Main() {
    for (int i=1; i<=10; i++) {
      Console.WriteLine("{0} ", i*i);
    }
  }
}
```

e anche in JavaScript

```
<html>
 <head>
  <title>Javascript Squares</title>
 </head>
 <body>
  <script>
   for (var i = 1; i <= 10; ++i)
   {
    document.write( Math.pow(i, i) + "<br>" );
   }
  </script>
 </body>
</html>
```

oppure in J

```
*:>:i.10
```

Bello, vero?

Nel mondo, le cose funzionano allo stesso modo. Qui a casa nostra diciamo "mangiare" in italiano, ma se sentiamo manicare, o anche pappare, o magnär o disnar, sappiamo che è la stessa cosa, solamente ci siamo spostati idealmente in Sardegna, in Emilia Romagna, in Veneto...

In sostanza: possiamo essere tutti italiani e dire le cose in tanti modi diversi. Oppure possiamo voler dire la stessa cosa in inglese, francese, tedesco... e lo possiamo fare tranquillamente. Il risultato è esattamente lo stesso, il modo di dirlo no.

Siamo procedurali o funzionali?

Volendo possiamo parlare come mangiamo. Potremmo dire a nostra sorella, o a nostro fratello o a nostra madre: "prendi una pentola, accendi il gas, metti su l'acqua e un po' di sale, se bolle allora butta la pasta, aspetta dieci minuti e scola" e avremmo descritto una procedura per arrivare al risultato: mangiare.

Oppure potremmo gridare semplicemente "mangiare!" e nostra sorella, o nostro fratello, o nostra, madre, sicuramente capirebbero: preparerebbero l'acqua, il sale, la pasta.... Il risultato sarebbe lo stesso.

Ecco qua, questo è più o meno quello che gli esperti chiamerebbero un linguaggio funzionale. Diciamo cosa fare e questo viene fatto.

Quindi siamo funzionali

Con i computer è la stessa cosa, ma a differenza delle sorelle quando diciamo fai così e cosà sono tanto stupidi da farlo veramente, per noi.

Se proviamo a fare un elenco di tutti i linguaggi di programmazione esistenti, otteniamo la bellezza di almeno cinquecento idiomi con cui dire a un computer cose deve fare. Qualcuno ne ha raccolti in quantità. Sono un'occasione unica per imparare

linguaggi differenti

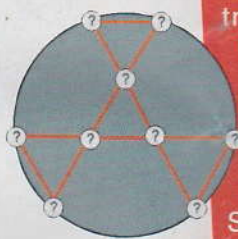
CYBERENIGMA SOFTWARE!

Non è certamente un vero cyberenigma, dei nostri in ultima pagina. Ma ci si avvicina... Dobbiamo piazzare le cifre da 1 a 9 sostituendo i punti di domanda, in modo che la somma di ogni triangolo sia 15 e la somma di tutte le cifre sulla circonferenza sia 30. Non possono esserci due cifre uguali.

Soluzione in Prolog:

```
solve(A, B, C, D, E, F, G, H, I) :-
  (
   between(1,9,A),
   between(1,9,B), B =\= A,
   between(1,9,C), C =\= B, C =\= A,
   between(1,9,D), D =\= C, D =\= B, D =\= A,
   between(1,9,E), E =\= D, E =\= C, E =\= B, E =\= A,
   between(1,9,F), F =\= E, F =\= D, F =\= C, F =\= B, F =\= A,
   between(1,9,G), G =\= F, G =\= E, G =\= D, G =\= C, G =\= B, G =\= A,
   between(1,9,H), H =\= G, H =\= F, H =\= E, H =\= D, H =\= C, H =\= B, H =\= A,
   between(1,9,I), I =\= H, I =\= G, I =\= F, I =\= E, I =\= D, I =\= C, I =\= B, I =\= A,
   A + B + G =:= 15,
   C + D + H =:= 15,
   E + F + I =:= 15,
   G + H + I =:= 15,
   A + B + C + D + E + F =:= 30
  ).
/*
 Call it from the Prolog command prompt as follows:
  ?- solve(A, B, C, D, E, F, G, H, I).
*/
```

Qualcuno riesce a fare di meglio, in altri linguaggi?

Anche con i computer, lo sappiamo bene, i modi di dire loro qualcosa sono veramente tanti. Ma quanti, in realtà? Probabilmente ne esistono anche molti di più, ma è certo che c'è chi ne ha messi in fila la bellezza di 164, se contiamo anche gli idiomi di uno stesso linguaggio (i dialetti, come sopra).

Anche in tal caso esistono moltissimi linguaggi procedurali, che quindi dicono al computer cosa fare passo per passo. Sono tutti quelli più conosciuti da tantissimi anni: dal Fortran al Pascal, dal Cobol al C.

Però possiamo fare la conoscenza con tanti linguaggi funzionali: Haskell, Hope, Moby, Pico, Scheme...

▲ *Parlare un linguaggio non significa per forza farlo con la bocca.*

Un sito che li parla tutti

All'indirizzo http://www.ntecs.de/old-hp/uu9r/lang/html/lang.en.html troviamo un intreccio di funzionalità fenomenale.

Per ciascuno dei 132 linguaggi presi in esame, una pagina li descrive brevemente e riporta i link dei linguaggi simili. Per esempio, sulla pagina del linguaggio Cilk sono indicati similari i linguaggi C, C#, C++, C-Talk, D, Java, Objective-C, Pike, TOM

Inoltre è indicato il sito di riferimento dove trovare il compilatore o le informazioni più approfondite.

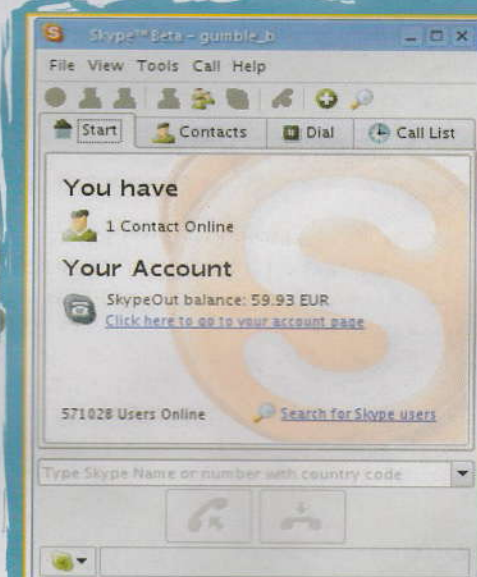
Impariamo dagli esempi

Sul sito in questione sono visibili anche dei brevi listati d'esempio, che ci permettono subito di farci un'idea della sintassi e della struttura dei singoli linguaggi.

Un paio di copia e incolla diventano uno strumento formidabile per chi è alle prime armi e vuole iniziare a capirci qualcosa, così come per chi è già esperto ma, forse, di Oz/Mozart non ne ha mai sentito parlare. Non c'è di meglio che vedere praticamente il modo di creare una routine che risolva cose semplici, per imparare come scrivere in un determinato linguaggio.

Skype: RIVOLUZIONE TELEFONICA

Skype usa la tecnologia del P2P non per scambiare file ma per parlarsi e – questa è la rivoluzione – telefonare.

La prima rivoluzione è stata il Web. La seconda è stata il peer-to-peer, con il Crollo dei Server Centrali (per parafrasare Asimov) e tutto il potere ai singoli utenti. La terza rivoluzione è appena cominciata ed è legata al P2P più di quanto sembri. Infatti Niklas Zennström e Janus Friis, i creatori di KaZaA, hanno avuto un'idea: portare la logica e la potenza del P2P nel mondo della telefonia. Così è nato Skype. Parlare a voce con gli utenti Skype di tutto il mondo è gratis; comporre il numero di un telefono ordinario invece è a pagamento,

▲ *L'interfaccia di Skype è veramente semplice. Con una carta di credito a disposizione è facile anche caricare il proprio account per chiamare telefoni normali. Per testare se la connessione funzione è possibile chiamare via Skype l'utente echo123, che non fa altro che ripetere quanto diciamo. Ma se c'è l'eco, funziona!*

IL TELEFONO VIA INTERNET SECONDO SKYPE

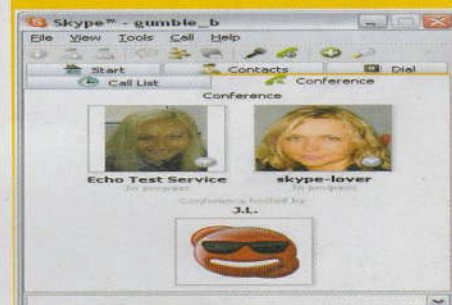
	Skype	Net2Phone	MSN M., ICQ, AIM, Yahoo M.	Altri client VoIP
Tempo di configurazione zero	Sì	No	No	No
Chiamate gratis senza limite per gli utenti dello stesso programma	Sì	No	Sì	Dipende
Qualità del suono	Come al telefono	Peggio che al telefono	Peggio che al telefono	Peggio che al telefono
Comunicazione cifrata per la massima privacy	Sì	No	No	No
Pubblicità zero	Sì	No	No	Dipende

ma con tariffe che iniziano a diventare interessanti. Se non è probabile che usiamo Skype per le chiamate urbane all'amica o a mammà per dirle di buttare la pasta che arriviamo, è invece certa la convenienza quando la chiamata diventa internazionale e assoluta per le intercontinentali.
Fare viaggiare la voce su Internet non è certo una novità. Ma Skype si usa su tutti i computer (Windows, Linux, Macintosh e persino palmari!) e questa sì che è una novità. Inoltre, e questo punto è fondamentale, Skype f-u-n-z-i-o-n-a. Gli altri servizi sono difficili da configurare e poi danno presso qualche problema. Questo no. L'importante è levarsi dalla testa l'idea che basti una connessione modem. Ci vuole minimo una ADSL, meglio se buona. Ma poi Skype si può usare davvero.

I segreti del telefono via P2P

Lavorando a KaZaA, il team di Skype ha imparato a meraviglia come sfruttare al massimo le risorse della rete e a fare viaggiare i dati nel modo più efficiente. Questa conoscenza, messa al servizio della telefonia, consente a Skype di raggiungere tassi di chiamate a buon fine e qualità di ascolto paragonabili a quelli della telefonia convenzionale (non cellulare), che ha un sacco di difetti, certo; ma novantanove volte su cento una telefonata raggiunge il destinatario, la linea non cade e si capisce tutto. Per la telefonia su Internet questi sono traguardi ancora lontani, che Skype finalmente raggiunge. L'esperienza sul P2P ha anche permesso al team di Skype di far funzionare il sistema a prescindere da NAT

▲ *Come i più moderni sistemi di messaggistica, anche Skype permette di associare una foto a un contatto.*

▼ *A una chiamata Skype possono partecipare fino a quattro persone!*

SKYPE CONTRO TELE2

Abbiamo messo a confronto la tariffa di chiamata telefonica di Skype contro quella di Tele2, che può essere considerata la più economica o una delle più economiche disponibili in Italia. I prezzi sono in euro. Gli addebiti alla risposta sono una tantum, quelli tariffari sono per ogni minuto di conversazione. Le tariffe di Tele2 sono ricavate da http://www.tele2.it/chap02/c020101.html, quelle di Skype da http://www.tele2.it/chap02 /c020101.html.

	SKYPE	TELE2	CHI VINCE
addebito alla risposta urbane	0	0,0619	Skype
addebito alla risposta interurbane	0	0,0775	Skype
addebito alla risposta cellulari	0	0,125	Skype
urbana diurna	0,02	0,011	Tele2
urbana serale e festiva	0,020	0,0058	Tele2
interurbana diurna	0,02	0,07	Skype
interurbana serale e festiva	0,02	0,02	Pari
cellulari diurna	0,288	0,218	Tele2
cellulari serale e festiva	0,288	0,141	Tele2

QUANTO COSTA TELEFONARE CON SKYPE

Le tariffe per alcuni Paesi europei e del mondo, in euro per minuto. L'elenco completo si trova a http://web.skype.com/skypeout/help.pricelist.html. Le chiamate di Skype sono sempre arrotondate al minuto intero, quindi parlare per dieci secondi è come parlare per un minuto.

Paese	Tariffa
Albania	0,158
Argentina	0,030
Belgio	0,020
Brasile	0,064
Canada	0,020
Cina	0,026
Cuba	0,957
Danimarca	0,020
Filippine	0,185
Filippine - Mobile	0,232
Finlandia	0,033
Francia	0,020
Giappone	0,031
Grecia	0,031
Groenlandia	0,537
Inmarsat	Non disponibile
Iraq	0,347
Irlanda	0,020
Israele	0,030
Italia	0,020
Italia - Mobile	0,288
Kenya	0,228
Libia	0,149
Lituania	0,105
Maldive	0,269
Malta	0,167
Marocco	0,240
Messico	0,092
Nuova Zelanda	0,020
Olanda	0,020
Polonia	0,030
Regno Unito	0,020
Repubblica Ceca	0,027
Romania	0,117
Russia	0,060
Spagna	0,020
Svezia	0,020
Svizzera	0,021
Taiwan	0,025
Thailandia	0,106
Ungheria	0,039
USA	0,020

e firewall e di allestire un sistema che si usa da subito, senza bisogno di configurazioni complicate.

Costa meno, ma costa

Se abbiamo parenti all'estero, un amore lontano, una telefonata di lavoro da fare oltreoceano Skype, costi alla mano, è una alternativa seria. Alla pagina http://web.skype.com/skypeout/ help.pricelist.html si può vedere l'elenco completo dei Paesi e delle tariffe. Dove non esiste una tariffa nazionale, Skype costa 0,017 euro al minuto; dove c'è, dipende. Chiamare l'Australia costa 0,020 euro al minuto, la Guinea-Bissau 1,009 euro al minuto. Si

possono chiamare anche i cellulari, per forza a tariffe più elevate. Telefonare a un cellulare in Germania costa 0,288 euro al minuto. Altra questione sono le chiamate locali. Chiamare l'Italia costa 0,020 euro al minuto (come l'Australia!) e chiamare un cellulare in Italia 0,288 euro al minuto (come la Germania!). Come mostriamo in una delle tabelle, su chiamate di lunghezza superiore al minuto una telefonata convenzionale, per il momento, tutto sommato conviene. Ma se Skype prenderà piede c'è da scommettere che le cose potrebbero cambiare.

I concorrenti

Ci sono svariati rivali di Skype nel campo della telefonia. Uno di questi è Net2Phone ma, a parte il fatto che è più rivolto alle aziende che ai singoli, le tariffe sono grosso modo il doppio di quelle di Skype. In più funziona solo su Windows e questo può essere un problema perché Windows ha il 90 percento del mercato, ma se la cugina australiana usa Linux è con quello che bisogna i conti (e la telefonata). In generale i concorrenti di Skype sono meno diffusi, costano di più oppure non funzionano su tutti, ma proprio tutti, i computer. Nessun costruttore di telefoni costruirebbe modelli che funzionano in quasi tutte le case, ma non tutte, no?

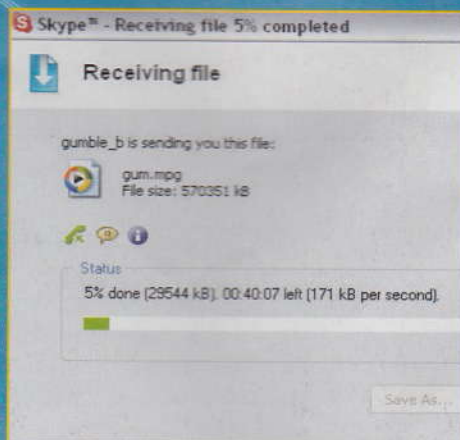
Pronto, Skype

Se abbiamo una buona connessione a Internet, consideriamo Skype. Parlare con gli altri Skypisti è gratis e telefonare all'estero costa meno. Il programma è gratis. Funziona su Windows, su Mac OS X, su Linux e sui palmari. Che altro serve per partire?

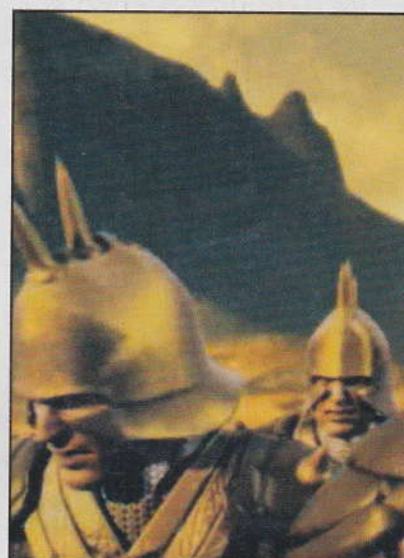
Reed Wright
reedwright@mail.inet.it

SKYPE CONTRO NET2PHONE

I prezzi sono in euro al minuto. I prezzi di Net2Phone sono forniti in dollari e quindi sono stati convertiti con qualche approssimazione, che però non altera la sostanza delle cose.
I dati precisi per Net2Phone si trovano a http://web.net2phone.com/italian/consumer/commcenter/, mentre quelli di Skype sono su http://web.skype.com/skypeout/help.pricelist.html.

	SKYPE	NET2PHONE
Canada	0,020	0,040
Filippine	0,185	0,175
Italia	0,020	0,050
Regno Unito	0,020	0,040
Spagna	0,020	0,050
USA	0,020	0,040

ENCICLOPEDIA dell'Hacking!

Attacco Diffing

"Il dipping è una semplice attacco che prevede il confronto di due file per ottenere informazioni preziose. Quali i vantaggi? Per esempio, se abbiamo a disposizione un file binario che contiene una password e non sappiamo in che posizione si trovi, possiamo farne una copia, modificare la pass e confrontarlo con il precedente: è intuibile che ci sarà almeno un byte che non corrisponde, così verremo a sapere la posizione della password.

ESEMPIO

Per l'esempio si cercherà di modificare il salvataggio di un gioco per ottenere il massimo dell'oro disponibile. Apriamo il gioco e notiamo l'oro: 7500 monete. Ora salviamo la partita: noi la chiameremo save1.gm1 per convenzione . Riapriamo il gioco e dirigiamoci al castello dove sono in vendita degli oggetti: compriamo il più economico (uno scheletro). Ora l'oro è a 7425 pezzi. Salviamo di nuovo come save2.gm1. Dirigiamoci verso la cartella dei salvataggi e di qui apriamo il prompt di MS-DOS e con i comandi 'cd nomecartella'. Digitiamo il comando 'fc /b save1.gm1 save2.gm1'. FC è l'utility che permette di confrontare due file, il parametro '/b' sta per il confronto binario e poi i nomi dei file da confrontare.

Ecco un possibile output:

```
C:\Programmi\MightAndMagicII\save>fc /b save1.gm1 save2.gm1

Confronto in corso dei file save1.gm1 e save2.gm1

000002A2: 31 32
000002C3: 32 FF
00000306: FF 03
00000368: 4C 01
00003ACE: FF 2F
00003AD3: 00 01
00003AE4: 08 07

C:\Programmi\MightAndMagicII\save>
```

Ora apriamo la calcolatrice di Windows e dal menù 'visualizza' scegliamo 'scientifica'. Premiamo il tasto 'Dec' e digitiamo 7500 (i pezzi dell'oro). Premiamo 'Hex' e otterremo il corrispondente esadecimale, ovvero : 1D4C ripetendo l'operazione con il valore 7425 (ovvero la cifra di monete disponibile dopo l'acquisto dello scheletro), otterremo 1D01. Scorrendo con lo sguardo gli indici notiamo la riga all'indirizzo 00000368 che contiene un valore che da 4C si è trasformato in 01 esattamente corrispondente ai pezzi dell'oro in esadecimale. Il passo successivo comporta la modifica del file. Apriamo dunque con un editor esadecimale il file save2.gm1 e modifichiamo l'offset (indirizzo) 00000368 dove si trova la cifra 1D01. Modifichiamo dunque il byte alla sinistra (1D) perché è il più significativo: mettendo FF (che rappresenta il massimo in esadecimale) si ottiene la quantità d'oro più grande possibile. Possiamo addirittura modificare il byte 01 per ottenere ancora più oro, sempre che il gioco lo permetta. Si potrebbe arrivare dunque anche a capire il significato degli altri byte trovati durante il confronto con MS-DOS, ma lasciamo il divertimento alla sperimentazione.

Requisiti

Un editor esadecimale qualsiasi e un gioco di ruolo o fantasy (nell'esempio Heroes of Might and Magic II).

Security

Alcuni giochi o programmi potrebbero usare tecniche come la compressioni di file 'delicati' e rendere impossibile lo sfruttamento di questa tecnica. Naturalmente è solo una esercitazione sperimentale e didattica, perché la modifica dei file sorgente di programmi commerciali è assolutamente vietata dalla licenza stessa

PER SCARICARE: technologismiki.com/hackman **ALTRI EDITOR:** www.bpsoft.com

Hash è un'operazione di cifratura di un intero testo, che genera una stringa di lunghezza fissa e che è univoca per quello specifico messaggio. Per esempio una stringa di 128 bit, che è associabile a quello specifico testo e a nessun altro. La probabilità che esista un'altra stringa identica per un messaggio diverso è inferiore a quella che ha un asteroide di colpirci ed eliminare la vita sul nostro pianeta...
Dalla stringa di lunghezza fissa che viene generata non è mai possibile risalire all'intero messaggio: si dice che è un sistema "one-way", a senso unico. È un'operazione usata per creare una specie di impronta digitale di un qualunque testo, così che ci possiamo accorgere di qualunque modifica, volontaria o no. È spesso usata quando scarichiamo un file, in modo tale da essere certi di avere recuperato bene tutto il file o che qualcuno non lo abbia nel frattempo sostituito o alterato.

ESEMPIO

Fastsum è un programma che funziona da riga di comando. Quindi, dopo averlo scaricato e installato, lo richiamiamo da Start > Esegui > cmd
Sulla riga di comando scriviamo fsum seguito dal percorso del file da cui vogliamo generare la stringa MD5. Se non specifichiamo altri parametri, la stringa è visualizzata a video. Altrimenti la possiamo salvare in un file, oppure possiamo inserire altri parametri seguendo il file di help che apriamo sul nostro browser dalla directory:
file://localhost/c:/Programmi/FastSum/How to use FastSum.htm

Alcuni famosi algoritmi di hashing sono:

SHA-1
È l'algoritmo di hash considerato più sicuro, se non abbiamo problemi di velocità di calcolo.

MD5
È un sistema di hashing estremamente diffuso, anche se non è il metodo più sicuro in assoluto. Se i dati sono veramente importanti, meglio SHA-1 che è inattaccabile.

RIPEMD
MD4
Algoritmi di hash utilizzati prima del duemila, ormai poco affidabili e superati.

Requisiti

Un programma veloce di generazione di controllo di stringhe hash secondo lo standard MD5, per esempio
http://www.fastsum.com/download/fsum-setup.exe

Security

Esistono strumenti software che ci consentono di controllare un intero sistema dalle possibili intrusioni, calcolando periodicamente una stringa hash per ogni file presente su un disco e quindi riconfrontando tutte le stringhe con quelle precedenti. Dove ci sono stringhe diverse, c'è stato un cambiamento del file e la traccia del tutto viene mantenuta in un database. L'analisi del database consente di evidenziare i cambiamenti significativi ed eventualmente pericolosi. Il progetto OpenSource Tripware che applica il tutto all'ambiente Linux lo troviamo a www.tripware.org.**d MD5,** per esempio:
http://www.fastsum.com/download/fsum-setup.exe

LINK:
Un veloce sistema di generazione di stringhe hash MD5, a riga di comando: www.fastsum.com
Il progetto OpenSource di controllo dell'integrità dei dati tramite hash: www.tripwire.org
La versione commerciale e per Windows del software tripware: www.tripware.com
Un semplice programma di controllo hash dell'integrità dei file masterizzati su CD: www.brandonstaggs.com/filecheckmd5.html

CYBERENIGMA

??

UN CIFRARIO DA FUMETTO: LE RISPOSTE

FINALMENTE, DOPO ERRORI DI STAMPA E LUNGHE ATTESE, LA RISPOSTA AL CYBERENIGMA DI HJ55!

Info...

Author
f3rr1gn0 13c0lp1
Scritto in...
java version 1.4.2_03-b02
"Dovunque vorremo andare andremo; una nave è questo in r...
non è solo una chiglia, uno scafo con un ponte e le vele.
Sì, una nave è fatta così; ma ciò che una nave è, è in realtà li...
JOHNNY DEPP- Pirates of the Caribbean
Per suggerimenti o insulti
f3rr1gn0@hush.com
CHIUDI

13c0lp1 in Java. Complimenti per il lavoro!

Le domande

PER TUTTI: chi è il personaggio dei fumetti con lo stesso nome del cifrario?
ESPERTI: dove si trova il cifrario su Internet?
GENI: qual è il messaggio segreto?

ESPERTI: si trova dovunque, per esempio a http://www.tonycrypt.com/Crittografia/Pigpen.htm.
GENI: il messaggio era pieghi zaini vuoti da bici qui al semaforo, che contiene tutte le lettere dell'alfabeto italiano.
SUPER HACKER: lo hanno fatto in cinque! E li troveremo sul CD del prossimo numero di Hackers Magazine…

Chi ha risposto!

PER TUTTI
CMOS (che non ci è riuscito, ma ha provato a fondo, bravo), primo arrivato!
nos (sorry, non Linus, Pigpen)

ESPERTI
Turk[z] (bravo)
Etabeta (continua a provare, è un bell'esercizio)

UN PO' DI SANO CODICE

La mail diceva di pubblicare solo l'allegato. Eccolo, vale un super hacker:

```
#/bin/sh
# SI CONSIGLIA UN FONT MONOSPAZIATO
# LE LETTERE ACCENTATE VANNO SCRITTE SENZA ACCEN
# PER BREVITA' HO OMESSO IL CONTROLLO SUGLI ARGOME
TI, FATE I BRAVI :)
# uso: ./cyberenigma-55.sh questa e la frase da cri
tare
# Sritto con VIM da natryum@hackerjournal.it che
annoiava sul treno.

while [ -n "$1" ]
do
l1=""
l2=""
l3=""
len=$((`expr length $1`
+ 1))
for (( i=1; $i<$len; i++))
do
w=`expr substr $1 $i 1`
case $w in

a)l1=`echo -n "$l1  |"`;
 l2=`echo -n "$l2  |"`;
 l3=`echo -n "$l3 --+"`;;
b)l1=`echo -n "$l1 | |"`;
 l2=`echo -n "$l2 | |"`;
 l3=`echo -n "$l3 +-+"`;;
c)l1=`echo -n "$l1 |  "`;
 l2=`echo -n "$l2 |  "`;
 l3=`echo -n "$l3 +--"`;;
d)l1=`echo -n "$l1 --+"`;
 l2=`echo -n "$l2  |"`;
 l3=`echo -n "$l3 --+"`;;
e)l1=`echo -n "$l1 +-+"`;
 l2=`echo -n "$l2 | |"`;
 l3=`echo -n "$l3 +-+"`;;
f)l1=`echo -n "$l1 +--"`;
 l2=`echo -n "$l2 |  "`;

 l2=`echo -n "$l2 |* "`
 l3=`echo -n "$l3 +--"`
p)l1=`echo -n "$l1 --+"`
 l2=`echo -n "$l2 *|"`
 l3=`echo -n "$l3  |"`;
p)l1=`echo -n "$l1 --+"`
 l2=`echo -n "$l2 *|"`
 l3=`echo -n "$l3  |"`
q)l1=`echo -n "$l1 +-+"`
 l2=`echo -n "$l2 |*|"`
 l3=`echo -n "$l3 | |"`
r)l1=`echo -n "$l1 +--"`
 l2=`echo -n "$l2 |* "`
 l3=`echo -n "$l3 |  "`
s)l1=`echo -n "$l1 \ /"`
 l2=`echo -n "$l2 \/ "`
 l3=`echo -n "$l3 U  "`
t)l1=`echo -n "$l1 \  "`;
 l2=`echo -n "$l2 >"`;
 l3=`echo -n "$l3 /  "`
u)l1=`echo -n "$l1  /"`;
 l2=`echo -n "$l2 <  "`;
  l3=`echo -ne "$l3
\\\"`;;
v)l1=`echo -n "$l1  ^ "`;
 l2=`echo -n "$l2 /\ "`;
 l3=`echo -ne "$l3 /
\\\"`;;
w)l1=`echo -n "$l1 \
```